UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

ANGELA ADKINS, on behalf of herself and all others similarly situated, Plaintiff, v. **EVEREST GLOBAL SERVICES, INC.,** Defendant.	Case No. Judge **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Angela Adkins ("Plaintiff") brings this Class Action Complaint, on behalf of herself and all others similarly situated (the "Class Members"), against Defendant Everest Global Services, Inc. ("Everest" or "Defendant") alleging as follows, based upon information and belief, investigation of her counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Everest's network that resulted in unauthorized access to highly sensitive data.[1] As a result of the Data Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

[1] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-13.pdf

2. Plaintiff and Class Members are individuals whose personally identifiable information ("PII") was acquired, stored, and utilized for Defendant's business and financial benefit.

3. The specific information compromised in the Data Breach includes PII, including full names and Social Security numbers.

4. Upon information and belief, prior to and through August 2022, Defendant obtained the PII of Plaintiff and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network.

5. Plaintiff's and Class Members' PII—which was entrusted to Defendant, its officials, and agents—was compromised and unlawfully accessed due to the Data Breach.

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of her and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown third party.

7. Defendant maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

8. In addition, upon information and belief, Defendant and its employees failed to properly monitor the computer network and IT systems that housed Plaintiff's and Class Members' PII.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals.

10. Defendant failed to provide timely, accurate and adequate notice to Plaintiff and Class Members. Plaintiff's and Class Members' knowledge about the PII Defendant lost, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendant's failure to warn impacted persons for approximately four months after first learning of the data breach.

11. In letters dated December 16, 2022, Defendant notified state Attorneys General and many Class Members about the widespread data breach that had occurred on Defendant's computer network and that Class Members' PII was accessed and acquired by malicious actors.[2]

12. In its required Notice Letter, Defendant "identified suspicious activity associated with its email environment."[3] Defendant became aware of the suspicious activity on August 15, 2022, but did not identify or notify the individuals who had their data stolen. After learning the identities of the affected persons, Defendant still waited months to notify state Attorneys General and Class Members about the widespread Data Breach.

13. Defendant acknowledged its investigation into the Data Breach determined that there was unauthorized access to email accounts between August 8, 2022, and August 16, 2022.

[2] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-13.pdf
[3] *Id.*

Defendant's investigation concluded and it learned what information was present in the accounts and lost to the data thieves on approximately October 10, 2022.

14. Defendant's Notice of Security further admitted that the PII accessed included individuals' names and Social Security numbers.

15. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

19. Accordingly, Plaintiff brings claims on behalf of herself and the Class for: (i) negligence, (ii) breach of implied contract; and (iii) unjust enrichment. Through these claims, Plaintiff seeks, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services.

THE PARTIES

20. Plaintiff Angela Adkins is a natural person, resident, and a citizen of the State of Ohio. Plaintiff Adkins has no intention of moving to a different state in the immediate future. Plaintiff Adkins is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Adkins's PII and owed her a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Adkins's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

21. Plaintiff received a notice letter from Everest dated December 16, 2022, stating that a data security incident occurred at Everest and that her personal information was involved in the incident.

22. Defendant Everest Global Services, Inc. is a provider of reinsurance and insurance, operating for decades years through subsidiaries in the United States, Europe, Singapore, Canada, Bermuda and other territories. Everest has is headquartered at 100 Everest Way, Warren, New Jersey 07059.

JURISDICTION AND VENUE

23. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

24. This Court has general personal jurisdiction over Defendant because Defendant maintains a principal place of business at 100 Everest Way, Warren, New Jersey 07059 regularly conducts business in New Jersey, and has sufficient minimum contacts in New Jersey. Defendant

intentionally availed itself of this jurisdiction by marketing and selling its services from New Jersey to many businesses nationwide.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANT'S BUSINESSES

26. Defendant Everest Global Services, Inc. is a provider of reinsurance and insurance, operating for decades years through subsidiaries in the United States, Europe, Singapore, Canada, Bermuda, and other territories.

27. On information and belief, in the ordinary course of insurance and reinsurance services, Defendant maintain the PII of customers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Photo identification;
- Medical information;
- Employment information, and;
- Other information that Defendant may deem necessary to provide its services.

28. Because of the highly sensitive and personal nature of the information Defendant acquire and store with respect to customers, Defendant, upon information and belief, promises to, among other things: keep PII private; comply with industry standards related to data security and

PII; inform customers of its legal duties and comply with all federal and state laws protecting customers' PII; and provide adequate notice to customers if their PII is disclosed without authorization.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

30. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

31. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

THE CYBERATTACK

32. On or around, August 15, 2022, Defendant became aware of suspicious activity in its network environment, specifically related to its email environment.

33. Defendant investigated the suspicious activity with the assistance of a third-party computer forensic expert.

34. Through investigation, Defendant determined that certain email accounts stored on its network and servers were subject to a cyber-attack that impacted its network where information on its network was accessed and acquired without authorization.

35. The investigation determined that files related to certain customers on Defendant's network were accessed and taken by an unauthorized user between August 8, 2022, and August 16, 2022.

36. Upon information and belief, Plaintiff's and Class Members' PII was exfiltrated and stolen in the attack.

37. Upon information and belief, the accessed systems contained PII and that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

38. It is likely the Data Breach was targeted at Defendant due to its status as provider of reinsurance provider that collects, creates, and maintains PII.

39. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

40. Defendant admitted that the stolen information may have included full names and Social Security Numbers.

41. While Defendant stated in the notice letter that the unusual activity occurred and was discovered on August 15, 2022, and was accessed for over a full week, Defendant failed to notify the specific persons or entities whose PII was acquired and exfiltrated until December 16, 2022– over four months later.

42. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiff's PII was stolen in the Data Breach. Plaintiff further believes her PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

43. As Defendant acknowledged in its Notice Letters, Defendant takes "the security of information is very important to us."[4]

[4] *Id.*

44. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

45. In response to the Data Breach, Defendant admits they worked with "computer forensic experts" to determine the nature and scope of the incident and purports to have taken steps to secure the systems. Defendant admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

46. Because of the Data Breach, data thieves were able to gain access to Defendant's IT systems for 8 days (between August 8, 2022, and August 16, 2021) and were able to compromise, access, and acquire the protected PII of Plaintiff and Class Members.

47. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

48. Plaintiff and the Class Members reasonably relied (directly or indirectly) on this sophisticated insurance institution to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

49. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Defendant negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

50. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the insurance industry and other industries holding significant amounts of PII preceding the date of the breach.

51. Two years ago, Defendant published a blog post on its website admitting that data breaches are prevalent, and that data protection is important[5], yet failed to adequately secure its systems and network to prevent the Data Breach.

52. In light of recent high profile data breaches at other insurance partner and provider companies, Defendant knew or should have known that their electronic records and customer PII would be targeted by cybercriminals and ransomware attack groups.

53. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[6] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[7]

54. In light of recent high profile cybersecurity incidents at other insurance partners and provider companies, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

[5] "Increasingly costly data breaches in recent years have shown the importance of data protection and privacy in the age of the data economy. While organizations have accelerated their pace in adapting to the increased levels of security and data sharing, much still needs to be done." Self-aware Data – Securing Data across its Life Cycle, Dec. 16, 2022: https://www.everestgrp.com/tag/data-breach/ (Last accessed on Dec. 29, 2022).
[6] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[7] *Id.*

55. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fail to Comply with FTC Guidelines

56. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

57. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[8] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[9]

58. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the

[8] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).
[9] *Id*.

network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. These FTC enforcement actions include actions against insurance providers and partners like Defendant.

61. Defendant failed to properly implement basic data security practices.

62. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

63. Defendant was at all times fully aware of its obligation to protect the PII of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

64. As shown above, experts studying cyber security routinely identify insurance providers and partners as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

65. Several best practices have been identified that at a minimum should be implemented by insurance providers like Defendant, including but not limited to: educating all employees; strong

passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

66. Other best cybersecurity practices that are standard in the insurance industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

67. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

68. These foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

DEFENDANT'S BREACH

69. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;

k. Failing to train all members of its workforces effectively on the policies and procedures regarding PII;

l. Failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

n. Failing to adhere to industry standards for cybersecurity as discussed above; and,

o. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

70. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted PII.

71. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

72. Cyberattacks and data breaches at insurance companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

73. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10]

[10] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

74. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

75. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

76. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

[11] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2022).

77. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

78. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[12]

79. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

80. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

81. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

---

[12] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[13] GAO Report, at p. 29.

82. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

83. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

84. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

85. PII can sell for as much as $363 per record according to the Infosec Institute.[14] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

86. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[15] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[16] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

---

[14] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[15] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).
[16] *Id* at 4.

87. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

88. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

89. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

90. Because of the value of its collected and stored data, the insurance industry has experienced disproportionally higher numbers of data theft events than other industries.

91. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

92. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

---

[17] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

93. Defendant has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

94. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

95. Plaintiff and Class Members' full names and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer network.

96. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

97. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

98. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

99. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

100. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

101. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

102. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members. Plaintiff has already experienced various phishing attempts by telephone and through electronic mail.

103. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

104. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

105. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer system and Plaintiff's and Class Members' PII. Thus, the Plaintiff and the Class Members did not get what they paid for and agreed to.

106. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

107. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

108. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

109. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

110. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Adkins' Experience

111. Plaintiff Adkins is very careful with her Private Information. She stores any documents containing PII a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. When Plaintiff does entrust a third-party with her PII, it is only because she understands the PII will be safeguarded in accordance with applicable privacy policies and state and federal law.

112. Plaintiff Adkins provided PII, including her Social Security number, to one of Defendant's clients as a condition of receiving services. Upon information and belief, Defendant thereafter acquired this PII and used it in furtherance to provide reinsurance services to one of Plaintiff Adkins current or former insurance companies.

113. Plaintiff Adkins first learned of the Data Breach after receiving a data breach notification letter dated December 16, 2022, from Everest, notifying her that Defendant suffered a data breach four months prior and that her PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

114. The data breach notification letter indicated that the PII involved in the Data Breach may have included Plaintiff Adkins' full name and Social Security number.

115. As a result of the Data Breach, Plaintiff Adkins made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

116. Plaintiff Adkins has spent multiple hours and will continue to spend valuable time for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

117. Plaintiff Adkins suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Adkins; (b) violation of her privacy rights; (c) the theft of her PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

118. As a result of the Data Breach, Plaintiff Adkins has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Adkins is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

119. As a result of the Data Breach, Plaintiff Adkins anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Adkins will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

CLASS ACTION ALLEGATIONS

120. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

121. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **All persons identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

122. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

123. Plaintiff reserves the right to amend or modify the Class or Subclass definitions as this case progresses.

124. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

125. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

126. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

127. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

128. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

129. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties,

conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

130. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

131. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

132. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

133. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

134. Defendant required individuals, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of insurance services.

135. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

136. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

137. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and patients, which is recognized by laws and

regulations, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

138. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

139. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

140. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

141. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

142. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

143. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

144. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

145. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members' PII.

146. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold vast amounts of PII, it was inevitable that

unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

147. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

148. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members—which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

149. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

150. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND COUNT
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

151. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

152. Plaintiff and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

153. Plaintiff and the Class were required to and delivered their PII to Defendant or Defendant's partners or business associates as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

154. Defendant, and its partners or business associates solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

155. Defendant accepted possession of Plaintiff's and Class Members' PII for the purpose of providing services to Plaintiff and Class Members.

156. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

157. In delivering their PII to Defendant and providing paying for insurance services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

158. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

159. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized insurance purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

160. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

161. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their PII to Defendant.

162. Defendant recognized that Plaintiff's and Class Member's PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

163. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

164. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PII as described herein.

165. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

166. Plaintiff repeats and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

167. This count is pleaded in the alternative to breach of implied contract.

168. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

169. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

170. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

171. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

172. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering insurance related services, a portion of which was to have

been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

173. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

174. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

175. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

176. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

177. Plaintiff and Class Members have no adequate remedy at law.

178. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

179. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

180. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FOURTH COUNT
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

181. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

182. Plaintiffs bring this claim for breach of third-party beneficiary contract against Defendant in the alternative to Plaintiff's claim for breach of implied contract.

183. Defendant entered into various contracts to provide insurance and reinsurance services to its clients.

184. These contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PII that Defendant agreed to collect and protect through its services. Thus, the benefit

of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

185. Defendant knew that if it were to breach these contracts with its insurance provider clients, the clients' customers and insureds, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

186. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

187. As reasonably foreseeable, Plaintiff and Class Members were harmed by Defendant's failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

188. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demand a trial by jury of any and all issues in this action so triable as of right.

Dated: January 3, 2023

Respectfully Submitted,

Vicki J. Maniatis
Vicki J. Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (865) 412-2700
vmaniatis@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
Email: gklinger@milberg.com

Terence R. Coates*
Justin C. Walker*
Jonathan T. Deters*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
jdeters@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

** Pro Have Vice Forthcoming*